

**REMARKS**

These remarks are directed to the final office action mailed January 9, 2008, setting a three month shortened statutory period for response set to expire on April 9, 2008. The office action issued by the Examiner and the citations referred to in the office action have been carefully considered.

Prompt reconsideration is requested in view of the above claim amendments and the following remarks. As indicated, amendments introduce no new matter.

**Claim Rejections under 35 USC § 101**

Claims 6 and 7 have been rejected under 35 USC §101 as being directed to non-statutory subject matter. Claim 6 has been amended to recite a “data carrier device comprising a computer program...” Support for amended claim 6 is found on page 4, lines 19-20. Claim 7 has been cancelled.

**Claim Rejections under 35 USC § 103**

Claims 1-2, 5-12, and 15-19 are rejected under 35 USC §103(a) as being unpatentable over Burger (U.S. Patent 6,219,439) in view of Trench (U.S. Patent Publication No. 2005/0154877 A1). Claims 3-4, 13-14, and 20-23 are rejected under 35 USC §103(a) as being unpatentable over Burger in view of Trench and in further view of Chen et al. (U.S. Patent 5,694,471).

Claims 1, 5, 6, and 8 recite a system and method:

“...for reading a document comprising a card provided with machine-readable holder details in a machine readable zone...”

The Examiner stated on page 8 of the January 9, 2008 office action that:

“Burger and Trench do not explicitly teach reading the machine readable holder details from a machine readable zone and checking the predetermined relationship of the data to the machine readable holder details.”

Chen et al. also does not teach reading machine readable holder details from a “machine readable zone” (MRZ). The sections in Chen et al. referenced by the Examiner (column 6, lines 50-54; column 7, lines 57-63; column 7, lines 18-29) only disclose performing a one-way hash function to obtain checksums for authenticating the card and do not teach or suggest an MRZ or obtaining readable holder details from the MRZ.

Claims 1, 5, 6, and 8 have been amended to recite a chip that contains:

“a biocertificate containing biometric data on the holder as well as data with a predetermined relationship to the machine readable holder details in the machine readable zone which predetermined relationship is based on a one-way function...”

The Examiner stated on page 8 of the January 9, 2008 office action that:

“Chen discloses a system wherein a card stores issuer identification information (holder details) and a key which it uses to perform a one-way hash function on the user information data (Chen: column 6, lines 50-54, column 7, lines 57-63) and then the authentication unit performs its own checksum on the issuer identification number and compares the results to authenticate the user (Chen: column 7, lines 18-29).”

Applicant respectfully submits that the Examiner’s statement is incorrect. The issuer identification information as taught by Chen et al. is not the same as the holder details as taught by Applicant. The issuer identification information is information regarding the entity issuing the card, **not the card holder**. Furthermore, Chen teaches performing a one-way hash function to obtain checksums for comparison “to authenticate the card” (column 7, line 22-23), **not the**

**user.** The user is authenticated by comparing a personal identification number with the personal identification number stored on the card (column 7, lines 23-26). Applicant teaches performing a one-way function on machine readable holder details to generate data and comparing the data to the machine readable holder details “to authenticate the machine readable holder details in the machine readable zone.” Authenticating the physical card is different from authenticating the holder details found in the MRZ.

Claims 1, 5, and 6 have also been amended to recite:

“establish[ing] the authenticity of the data in the biocertificate by receiving digitally signed biocertificate data that is obtained by digitally signing said data in said biocertificate by said chip using one of said one or more private keys and checking the digitally signed biocertificate data with the certificate from said issuing authority...”

Trench discloses authenticating the chip with a challenge-response technique, but does not disclose **authenticating the biocertificate data** stored in the chip. Burger also does not disclose authenticating data stored in the chip. Instead, Burger discloses authenticating the user, by confirming that the fingerprint data in the chip is equal to the fingerprint data as received from the fingerprint scanner.

On page 9 of the January 8, 2008 office action, the Examiner states that “Burger discloses a key that is stored on the card” to support the Examiner’s view that Chen et al.’s teachings can be easily applied in Burger. However, the Examiner fails to show where Burger discloses such a key. Applicant was unable to find support for this statement in Burger.

None of the documents disclose authenticating biometric data in the chip. Moreover, none of the documents disclose authenticating the holder details in the MRZ via two steps, i.e., first authenticating the holder details in the chip and then checking the one-way functional relationship with the holder details in the MRZ. All the references fail to teach or suggest

authenticating the holder details in the MRZ of the card by also authenticating the data related thereto stored in the chip.

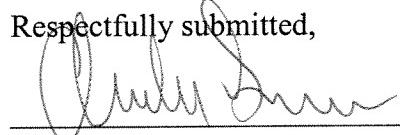
Thus, by means of the claimed features, it is possible to securely check that the document with the chip is authentic, the data in the chip is authentic, the holder details in the MRZ of the document are authentic, and that the person presenting the document is really the holder of the document.

Combining Burger, Trench, and Chen in any manner does not result in the claimed limitations and elements of Applicant's invention. Applicant submits that the independent claims and the claims thereby dependent thereon are not obvious and are therefore patentable under 35 USC §103. The Examiner is respectfully requested to reconsider and now withdraw the Examiner's rejection.

In view of the above, it is respectfully submitted that this application is now in good order for allowance, and such early action is respectfully solicited. Should matters remain, which the Examiner believes could be resolved in a telephone interview, the Examiner is requested to telephone Applicant's undersigned attorney.

The Director is authorized to charge any additional fee(s) or any underpayment of fee(s), or to credit any overpayments to **Deposit Account Number 50-2638**. Please ensure that Attorney Docket Number 072998-012200 is referred to when charging any payments or credits for this case.

Respectfully submitted,



Charles Berman  
Reg. No. 29,249

Date: April 8, 2008

GREENBERG TRAURIG, LLP  
2450 Colorado Avenue, Suite 400E  
Santa Monica, CA 90404  
Phone: (310) 586-7700  
Fax: (310) 586-7800  
E-mail: laipmail@gtlaw.com  
LA 127,193,403v1